Claims

WHAT IS CLAIMED IS:

1. A method to manage secure communications, comprising:

establishing a secure session on a secure site with an external client that communicates from an insecure site;

detecting access attempts during the session directed to potentially insecure transactions; and

transparently managing the access attempts by inspecting the access attempts before making them available to the external client.

2. The method of claim 1 wherein the detecting further includes translating non-secure links into secure links for the insecure transactions before presenting results of the access attempts to the external client.

3. The method of claim 1 further comprising:

identifying the potentially insecure transactions as attempts by the external client to view a World-Wide Web (WWW) browser page having insecure Hypertext Transfer Protocol (HTTP) reference links or File Transfer Protocol (FTP) reference links embedded therein, and wherein the reference links reside within the secure site; and

suppressing normally occurring security warning messages associated with the reference links, preventing the external client from viewing the security warning messages.

4. The method of claim 1 further comprising:

identifying the potentially insecure transactions as attempts by the external client to activate one or more external reference links from a World-Wide Web (WWW) browser page, wherein the external reference links are associated with external sites not controlled by the secure session and not secure; and

using a proxy on behalf of the external client during the secure session in order to access the external sites and making transactions with the external sites appear secure to the external client during the secure session.

5. The method of claim 1 further comprising:

identifying the potentially insecure transactions as attempts by the external client to activate one or more external reference links from a World-Wide Web (WWW) browser page, wherein the external reference links are associated with external sites not controlled by the secure session;

inspecting content or metadata of the content associated with the external reference links in advance of providing the external reference links to the external client; and

taking zero or more actions based on the inspection before the external reference links are visible, if at all, to the external client during the secure session.

6. The method of claim 5 wherein the taking of the zero or more actions further includes at least one action that is at least one or more of:

permitting normally occurring security warnings to present messages to the external client by taking no action;

removing the external reference links from a browser page that originally included the reference links before presenting the browser page to the external client, thereby preventing external client access to the external reference links;

generating for and displaying to a custom warning message that is presented to the external client;

issuing alerts, notifications, or advisories to a monitoring entity or log; and

determining the external reference links are low-risk to or trusted by the secure site and thereby suppressing normally occurring security warnings from being presented to the external client.

7. The method of claim 5 wherein the inspecting the content further includes using a proxy on behalf of the external client during the secure session for

performing the inspecting.

8. A method to manage secure communications, comprising:

detecting potentially insecure transactions occurring during a secure session, wherein the insecure transactions result from actions requested by an external client participating in the secure session;

inspecting the potentially insecure transactions in advance of satisfying the actions requested; and

making a determination for at least one of the following: permitting the insecure transactions to proceed unmodified by performing the actions requested for the external client, permitting the insecure transactions to proceed in a modified fashion, and denying the insecure transactions by denying the actions requested.

9. The method of claim 8 wherein the inspecting further includes, identifying the potentially insecure transactions as a request by the external client to access a World-Wide Web (WWW) browser page having embedded reference links to other browser pages that reside within an environment of the secure session, wherein the reference links are modified in order to suppress normally occurring security warning messages when the browser page is presented to the external client.

10. The method of claim 9 wherein the making a determination further includes, permitting the insecure transactions to proceed in the modified fashion by changing the reference links from Hypertext Transfer Protocol (HTTP) insecure links to HTTP over Secure Sockets Layer (HTTPS) in order to suppress the security warning messages.

11. The method of claim 8 wherein the inspecting further includes, identifying the potentially insecure requests as an external client access attempt to reference an external site outside the control of the secure session.

12. The method of claim 11 wherein the making a determination further includes permitting the insecure transactions to proceed unmodified by permitting normally occurring security warnings to be presented to the client before satisfying the external client access attempt to reference the external site.

13. The method of claim 11 wherein the making a determination further includes permitting the insecure transactions to proceed in a modified fashion by transparently processing the external client access attempt within a proxy making the external client access attempt appear to be part of the secure session.

14. The method of claim 11 wherein the making a determination further includes denying the insecure transactions after determining that the external client access attempt is corrupted and notifying the external client of the denial.

15. The method of claim 11 wherein the making a determination further includes denying the insecure transactions after determining that the external client access attempt is corrupted and logging information about the external client access attempt.

16. A secure communications management system, comprising:

a secure communications manager that manages a secure session with an external client associated with an insecure site; and

a proxy that interacts with the secure communications manager in order to inspect potentially insecure communications requested by the external client during the secure session, and wherein the proxy selectively processes the potentially insecure communications on behalf of the external client within the secure session.

17. The secure communications management system of claim 16 wherein the secure communications manager translates Hypertext Transfer Protocol (HTTP) insecure communications into HTTP over Secure Sockets Layer (HTTPS) secure communications during the secure session.

18. The secure communications management system of claim 16 wherein the proxy selectively modifies a number of the potentially insecure communications and permits them to proceed thereby suppressing normally occurring security warning messages that the secure communications manager issues.

19. The secure communications management system of claim 16 wherein the proxy selectively leaves a number of the potentially insecure communications unchanged and permits secure communications manager to issue security warning messages to the external client.

20. The secure communications management system of claim 16 wherein the proxy selectively denies a number of the potentially insecure communications to proceed and at performs at least one of reports the denial to another entity and records the denial in a log.

21. The secure communications management system of claim 16, wherein the proxy selectively issues custom warning messages or explanations to the external client regarding a number of the potentially insecure communications.

22. A secure communications management system, comprising:

a secure session; and

secure reference links accessible within the secure session; and

potentially insecure reference links accessible from the secure session;

wherein an external client associated with an external site establishes the secure session with a secure site, the external client references the secure reference links and the potentially insecure reference links during the secure session, and wherein the potentially insecure reference links are inspected and modified in advance of being made available to the external client during the secure session.

23. The secure communications management system of claim 22 further comprising a proxy that inspects and modifies the potentially insecure reference links in advance of making them available to the external client during the secure session.

24. The secure communications management system of claim 22 wherein the secure session is represented within a Word-Wide Web (WWW) browser that the external client uses for interacting with the secure site.

25. The secure communications management system of claim 22 wherein the potentially insecure reference links are transparently modified into a number of the secure reference links before being made available to the external client during the secure session.

26. The secure communications management system of claim 22 wherein a number of the potentially insecure reference links are processed by a proxy on behalf of the external client and appear to the external client to be a number of the secure reference links.

27. The secure communications management system of claim 22 wherein normally occurring security warning messages associated with a number of the potentially insecure reference links are suppressed and not visible to the external client during the secure session.

28. The secure communications management system of claim 22 wherein a number of the potentially insecure reference links are not made available to the external client during the secure session.

29. The secure communications management system of claim 22 wherein a number of the potentially insecure reference links generate notifications to external entities.

30. The secure communications management system of claim 22 wherein a number of the potentially insecure reference links generate written messages to a security log.